ENVISTA FORENSICS

United States vs. Jamarr Smith, et al.

3:21-CR107-NBB-RP

Spencer J. McInvaille CTNS, CWA, CCO, CCPA

Digital Forensic Examiner and Cellular Analyst

2700 Gateway Centre Blvd, Suite 100

Exhibit "D"

Qualifications

I am currently a Technical Lead with Envista Forensics in Morrisville, North Carolina. In this capacity, I provide consulting and analytical services to defense attorneys, prosecutors, and plaintiff attorneys in the practice of mobile device forensics. Coming from a law enforcement background, I have analyzed call detail records and historical cell site location information, performed mobile device extractions, and have rendered conclusions pertaining to criminal cases. I have also performed those same duties in my capacity with Envista Forensics. I am a Certified Telecommunications Network Specialist (CTNS) and a Certified Wireless Analyst (CWA). I am also a Cellebrite Certified Operator (CCO) and a Cellebrite Certified Physical Analyst (CCPA). I have extensive training and experience analyzing location data such as call detail records, global positioning data, mobile device forensics, mobile networks, wireless communications, and rendering opinions about these data types. I have qualified and testified as an expert over 35 times in State and Federal Courts in the following states: California, Florida, Illinois, Maryland, Michigan, Minnesota, Missouri, North Carolina, New Jersey, South Carolina, Texas, and Virginia. My expert testimony has included the areas of Historical Cell Site Analysis, Global Positioning System, Google Location History, and Mobile Device Forensics. I have testified in both State and Federal Courts in reference to Google Geofence warrants.

Geofence Warrant Process Overview

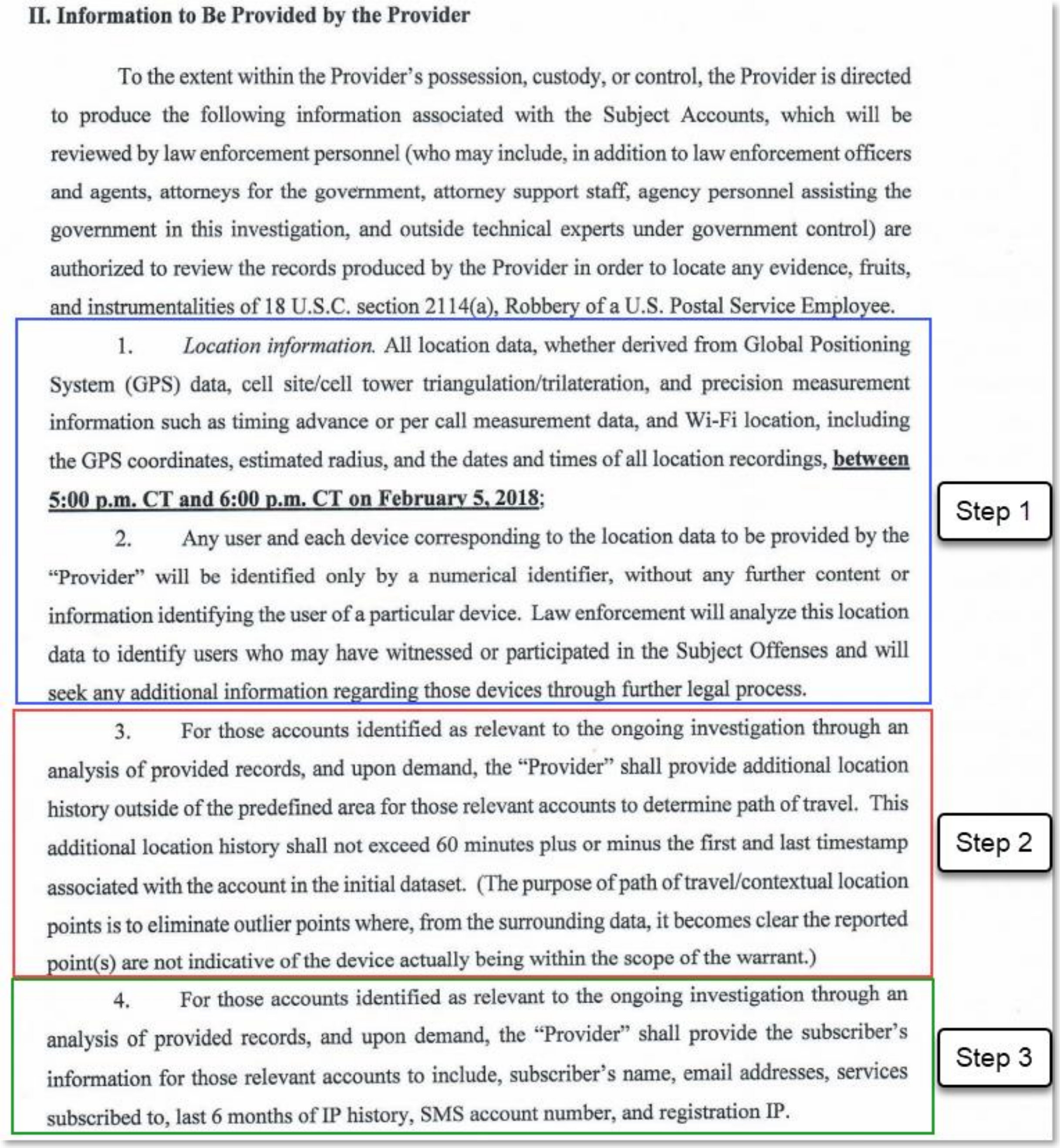
Google Geofence Warrants provide locations associated with devices belonging to Google account users with Location History enabled. Location History is a service of Google, which Google has described as a personal and private journal of the user's locations. This is not to be confused with location services on mobile devices, which refers to the device-based settings such as those you see when choosing whether to use airplane mode or not. Location History is an account-level setting allowing data to be collected across any devices with the account logged in. Google states Location History allows the user to better tailor searches and enhance their user experience.

Geofence warrants demand Google search their databases so law enforcement can locate unknown suspects. Google states this search requires them to search their entire database containing Location History to locate any users within an area prescribed by law enforcement. Google has contended this search is performed only when demanded by law enforcement and is not a normal business function. All user accounts with Location History are queried for Google to respond to the warrant. This large-scale search occurs because all Location History is stored in a database and identified with individual device IDs. These details are described by Google employee Marlo McGriff in a declaration filed in other geofence cases, March 11, 2020. (Marlo McGriff declaration, Attachment I) Google has quantified the number of accounts searched for each geofence in a declaration. *"In October 2018, there were approximately 592 million daily active users of Location History worldwide. Roughly one-third of all active Google users had Location History enabled on their accounts."* (Emily Mosley declaration, March 4, 2022, Attachment II). This means for each geofence contained within a single warrant, approximately 592 million accounts are searched to determine whether they contain responsive data to the warrant.

Case Specific Analysis

The geofence warrant, in this case, is broken down into three steps. Figure 1 color codes each step as they were directed in the warrant affidavit written by Inspector Todd Matney of the United States Postal Inspection Service and the area described to be searched.

Figure 1.



II. Information to Be Provided by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts, which will be reviewed by law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of 18 U.S.C. section 2114(a), Robbery of a U.S. Postal Service Employee.

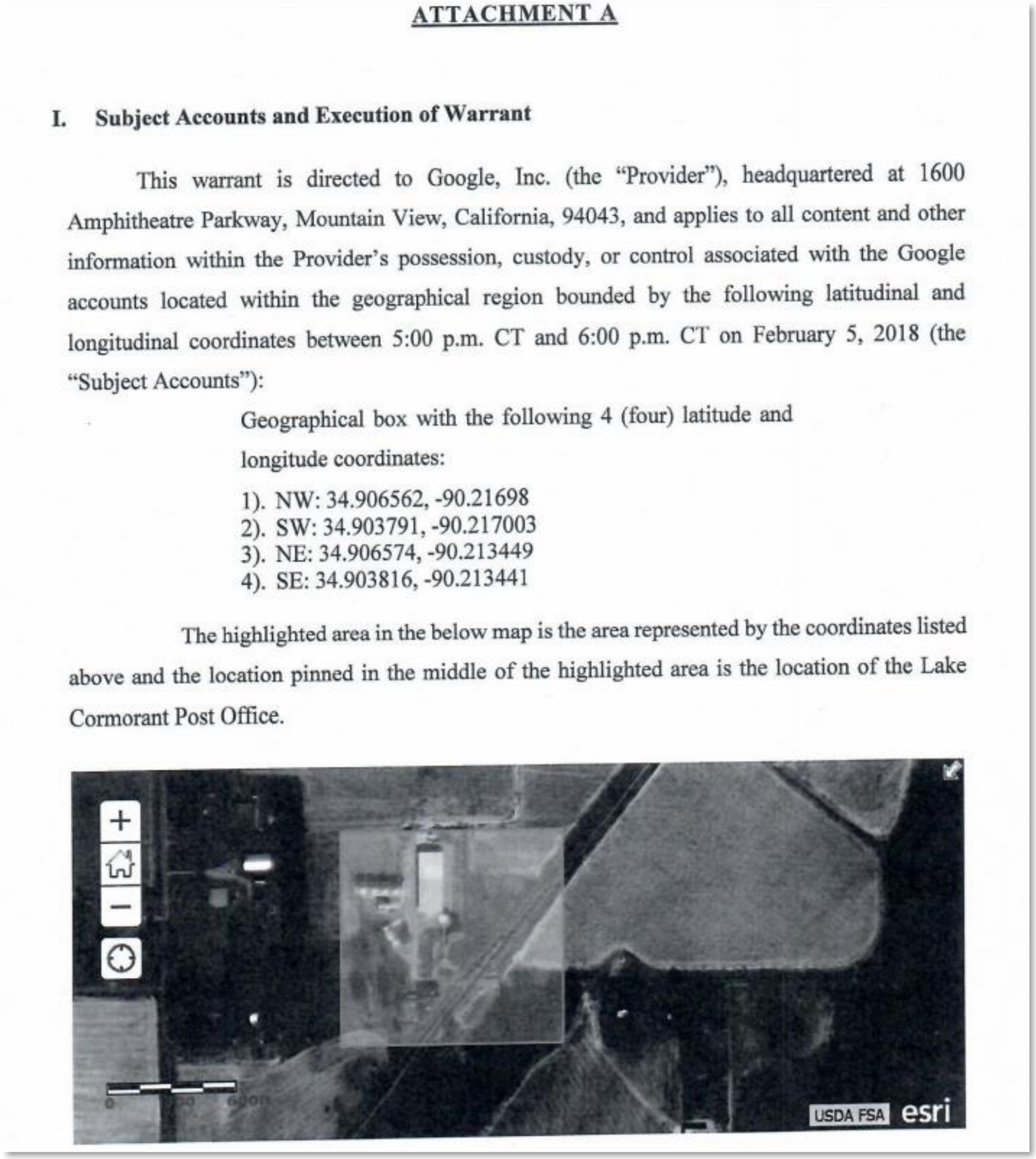
1. *Location information.* All location data, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location, including the GPS coordinates, estimated radius, and the dates and times of all location recordings, **between 5:00 p.m. CT and 6:00 p.m. CT on February 5, 2018**;

2. Any user and each device corresponding to the location data to be provided by the "Provider" will be identified only by a numerical identifier, without any further content or information identifying the user of a particular device. Law enforcement will analyze this location data to identify users who may have witnessed or participated in the Subject Offenses and will seek any additional information regarding those devices through further legal process.

3. For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, the "Provider" shall provide additional location history outside of the predefined area for those relevant accounts to determine path of travel. This additional location history shall not exceed 60 minutes plus or minus the first and last timestamp associated with the account in the initial dataset. (The purpose of path of travel/contextual location points is to eliminate outlier points where, from the surrounding data, it becomes clear the reported point(s) are not indicative of the device actually being within the scope of the warrant.)

4. For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, the "Provider" shall provide the subscriber's information for those relevant accounts to include, subscriber's name, email addresses, services subscribed to, last 6 months of IP history, SMS account number, and registration IP.

Figure 1 cont.



ATTACHMENT A

I. Subject Accounts and Execution of Warrant

This warrant is directed to Google, Inc. (the "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043, and applies to all content and other information within the Provider's possession, custody, or control associated with the Google accounts located within the geographical region bounded by the following latitudinal and longitudinal coordinates between 5:00 p.m. CT and 6:00 p.m. CT on February 5, 2018 (the "Subject Accounts"):

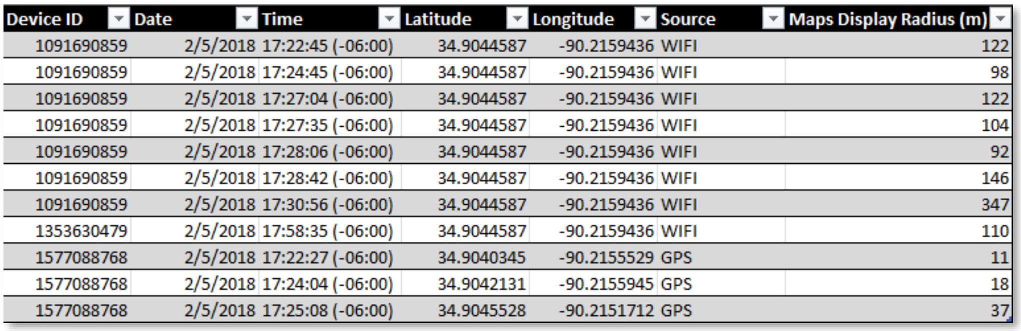
Geographical box with the following 4 (four) latitude and longitude coordinates:

1). NW: 34.906562, -90.21698
2). SW: 34.903791, -90.217003
3). NE: 34.906574, -90.213449
4). SE: 34.903816, -90.213441

The highlighted area in the below map is the area represented by the coordinates listed above and the location pinned in the middle of the highlighted area is the location of the Lake Cormorant Post Office.

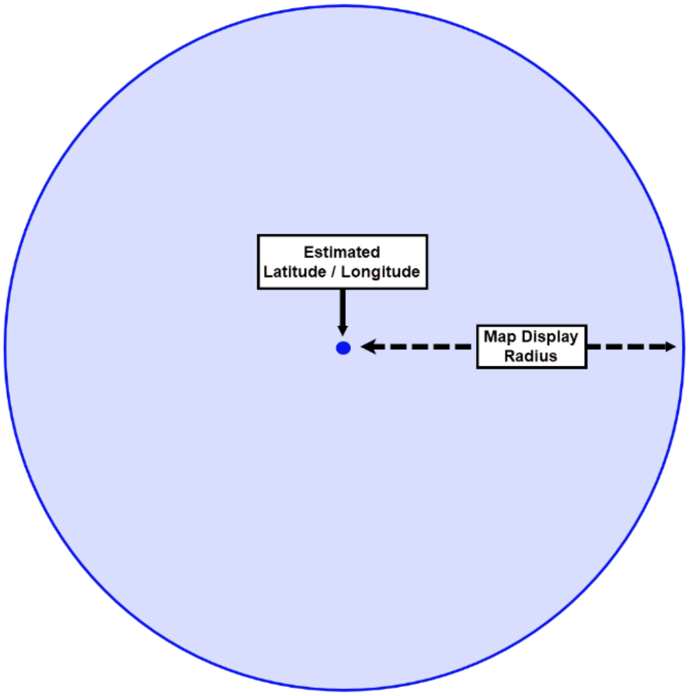
Step 1 requires Google to search approximately 592 million accounts with Location History to determine which users were within the boundaries during the time constraints of the "initial search parameters" prescribed by the affiant. Those device IDs and their estimated location within the geofence were returned in a spreadsheet, “21657812.Location040419.csv”. This spreadsheet lists each of the device IDs and their locations. Each row indicates the device, date/time, latitude and longitude, the source used for the estimate, and the maps display radius or confidence. (Figure 2 is an example of the data returned). The maps display radius is indicated in meters and the radius is drawn around the center point referenced with the latitude and longitude. (Figure 3 is an example of the maps display radius). Google estimates the device should be located within the circle and states their goal is for that to be true 68% of the time. (Declaration Marlo McGriff, March 11, 2020)

Figure 2



Device ID	Date	Time	Latitude	Longitude	Source	Maps Display Radius (m)
1091690859	2/5/2018	17:22:45 (-06:00)	34.9044587	-90.2159436	WIFI	122
1091690859	2/5/2018	17:24:45 (-06:00)	34.9044587	-90.2159436	WIFI	98
1091690859	2/5/2018	17:27:04 (-06:00)	34.9044587	-90.2159436	WIFI	122
1091690859	2/5/2018	17:27:35 (-06:00)	34.9044587	-90.2159436	WIFI	104
1091690859	2/5/2018	17:28:06 (-06:00)	34.9044587	-90.2159436	WIFI	92
1091690859	2/5/2018	17:28:42 (-06:00)	34.9044587	-90.2159436	WIFI	146
1091690859	2/5/2018	17:30:56 (-06:00)	34.9044587	-90.2159436	WIFI	347
1353630479	2/5/2018	17:58:35 (-06:00)	34.9044587	-90.2159436	WIFI	110
1577088768	2/5/2018	17:22:27 (-06:00)	34.9040345	-90.2155529	GPS	11
1577088768	2/5/2018	17:24:04 (-06:00)	34.9042131	-90.2155945	GPS	18
1577088768	2/5/2018	17:25:08 (-06:00)	34.9045528	-90.2151712	GPS	37

Figure 3



The affiant states in step 1 that "Law enforcement will analyze this location data [21657812.Location040419.csv] to identify users who may have witnessed or participated in the Subject Offenses and will seek any additional information regarding those devices [Device IDs] through further legal process" (November 8, 2018 Google Search Warrant, Matney), which requires an analysis of the step 1 data and for law enforcement to decide which Device IDs they wish to receive additional Location History on (steps 2 & 3). Step 1, in this case, located three device IDs.

Step 1 in this case uses a geofence referenced in the search warrant with 4 geolocation points to create a square shape. This geofence covers approximately 98,192 square meters. Due to the manner in which Google acquires these location estimates and then reports them as responsive, devices have often been returned as responsive even when the device was outside of the geofence. This is because the device can be located anywhere within the blue circle reference in Figure 2. In figure 4 (below) you can see the geofence requested and in figure 5 (below) you can see one of the responsive data points from the search warrant step 1 return.

Figure 4.

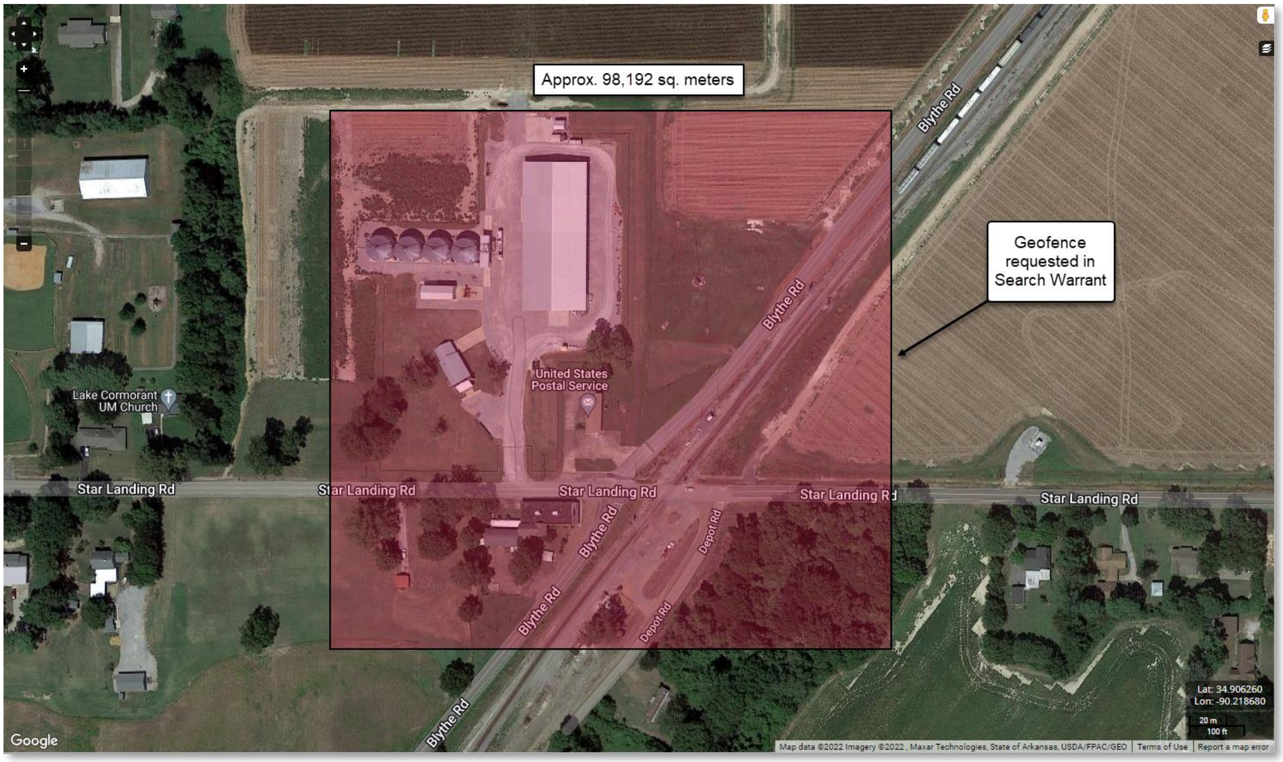
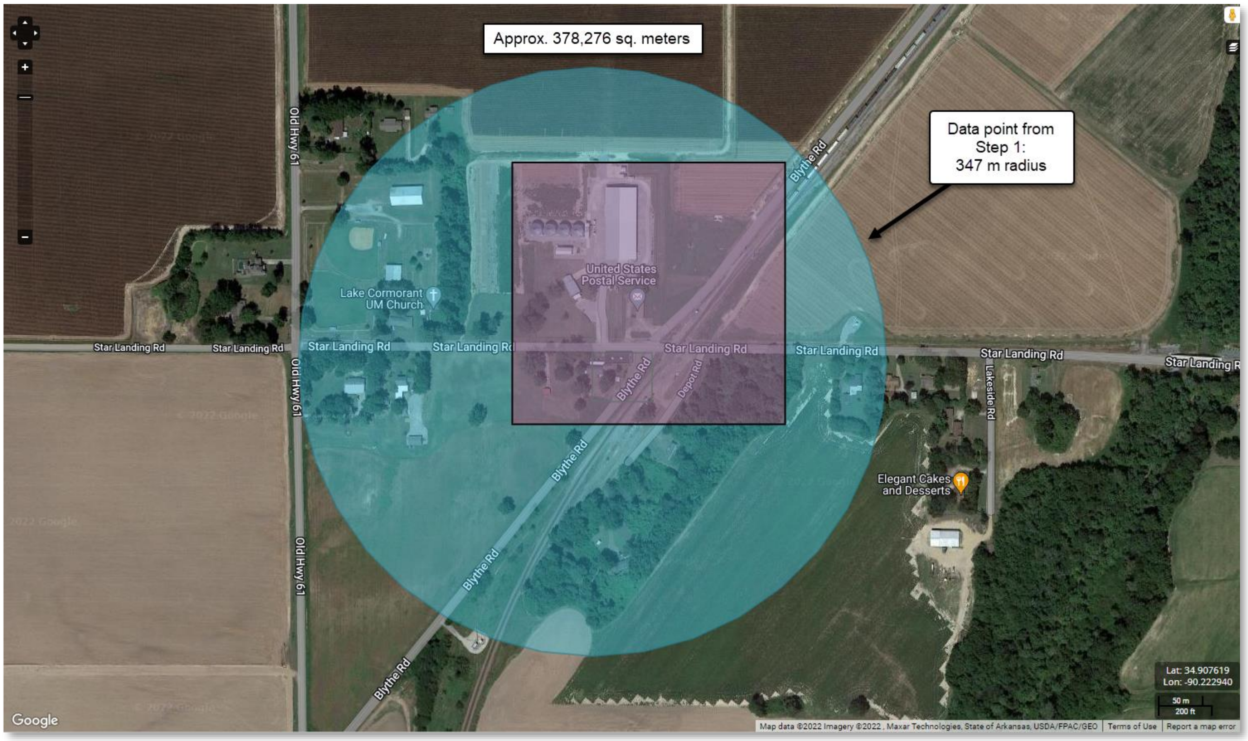


Figure 5.


Approx. 378,276 sq. meters
Data point from Step 1: 347 m radius
Blythe Rd
Old Hwy 61
United States Postal Service
Lake Cormorant UM Church
Star Landing Rd
Depot Rd
Lakeside Rd
Elegant Cakes and Desserts
Lat: 34.907619
Lon: -90.222940
50 m
200 ft
Google
Map data ©2022 Imagery ©2022 , Maxar Technologies, State of Arkansas, USDA/FPAC/GEO
Terms of Use
Report a map error

The data point in figure 4 is a responsive data point returned in this case. It is a 347-meter display radius encompassing the geofence and surrounding areas. Based on documentation from Google, this device could be located anywhere within the blue circle. Further, based on Google's representatives, the device could also be located outside of this circle. Making the search area more than three times larger than what is depicted by the warrant and shown in figure 3.

Step 2 is a request for contextual data. In step two, a request for additional Location History allows for data to be received that is outside of the initial search parameters. The data can show the devices before and after they were indicated as responsive in the step 1 data.

Sarah Rodriguez, with Google, describes when step 2 data is provided in her declaration dated March 11, 2020. Rodriguez stated, "Second, the government reviews the de-identified production version to determine the device numbers of interest. If additional de-identified location information for a device in the production is necessary to eliminate false positives or otherwise determine whether that device is relevant to the investigation, law enforcement can compel Google to provide additional contextual location coordinates beyond the time and geographic scope of the original request (if authorized in that request)." Rodriguez stated further, "Finally, based on the de-identified data produced, the government can compel Google (if authorized in the request) to provide account-identifying information for the device numbers in the production that the government determines are relevant to the investigation. In response, Google provides account subscriber information such as the email address associated with the account and the name entered by the user on the account." (Sarah Rodriguez declaration, Attachment III)

Step 2 data was not contained in the discovery and appears to have been skipped.

Step 3 is a request for Subscriber information. In step 3, three device IDs were requested for subscriber information or to be "de-anonymized." This data was provided with, "Letter 2165781" and provided the following files, "2165781.Key.csv", "bleek2004.AccountInfo.txt", "jamarrsmith33.AccountInfo.txt" and "permanentwavesrecords.AccountInfo.txt". Theses files were provided in response to, "Search Warrant dated November 8, 2018 (Google Ref. No. 2165781) Case No.: 3:18MJ007-RP". Google provided both step 1 and step 3 data as a result of the warrant dated, November 8, 2018.

Conclusions

I have analyzed the Google geofence warrant, the responsive data to that warrant. Based on the search warrant dated November 8, 2018, the warrant requested the data relevant to the initial search parameters (step 1) and Google returned the following file, "21657812.Location040419.csv". This data contained 3 Device ID's.

Additional information for all three Device IDs in step 1 was provided June 10, 2019. Google provided subscriber information as described in the November 8, 2018, Google Search Warrant. This data was accompanied by a response letter, "Letter 2165781" which advised the response was in regard to, "Search Warrant dated November 8, 2018 (Google Ref. No. 2165781) Case No.: 3:18MJ007-RP".

While assisting counsel in this matter, I requested all emails or correspondence between Law Enforcement and Google related to these requests. In my experience, there are communications for these requests and these communications provide significant insight into the process by which data was requested and responded to. I have not been provided with any of those communications as of the date of this report.

It is my professional opinion that approximately 592 million Google accounts were searched to provide the Government 3 device identifiers listed in step 1 data return. Google has documented they cannot complete a search to locate responsive data without searching all accounts. This search occurs no matter the size, shape, or timeframes provided within the warrant. Further, based on the data contained, the effective range of the geofence was larger than directed in the warrant request due to the manner in which data was requested by the Government. Lastly, both step 1 and step 3 data sets were provided in response to one single warrant, despite the affiant stating, "…[law enforcement] will seek any additional information regarding those devices [Device IDs in step 1] through further legal process". As written, an additional warrant was needed to obtain the subscriber information (step 3). The conclusions and opinions are based on my experience in Google geofence warrants, the analysis of responsive data and the documents in this case.

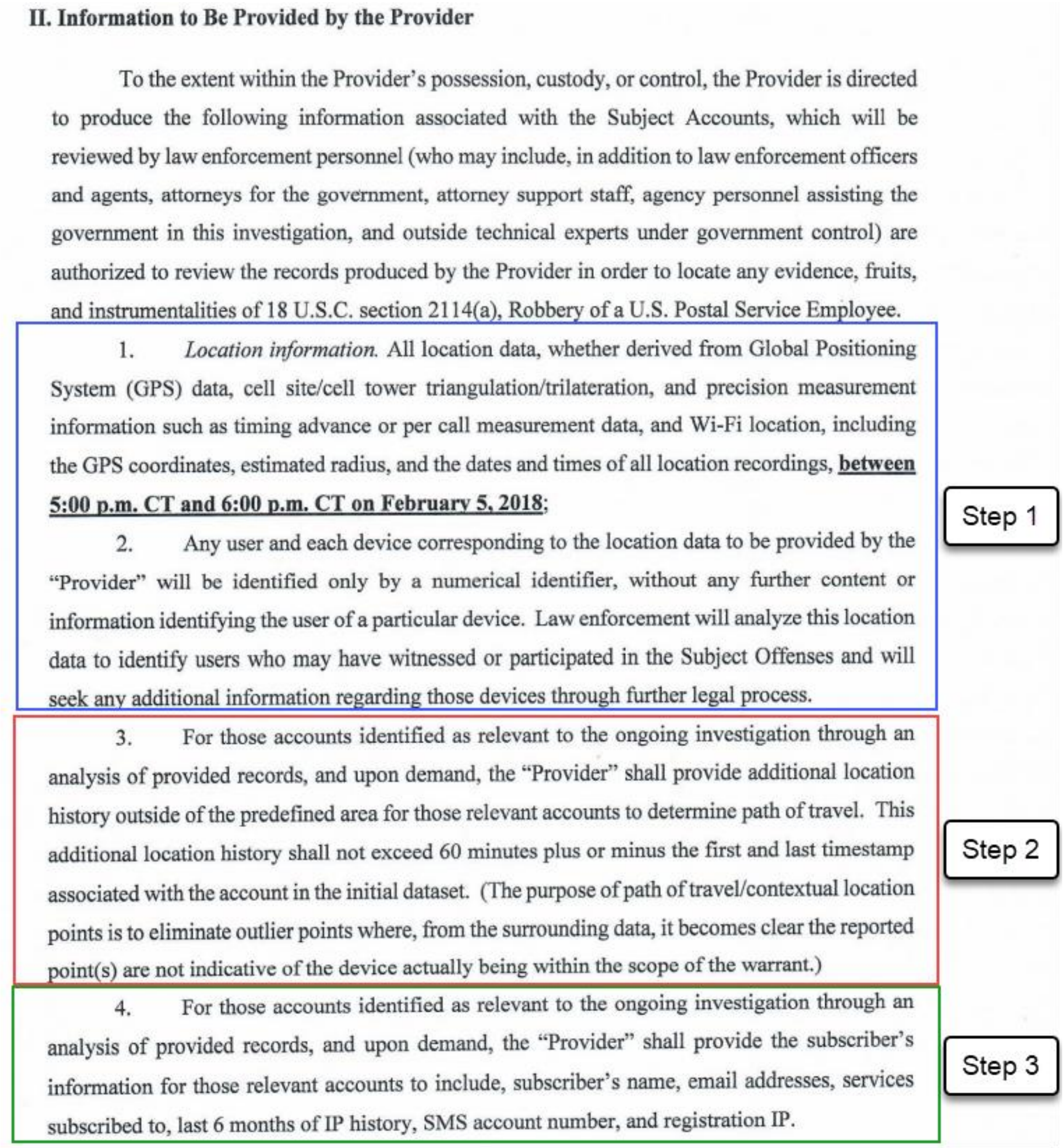
Spencer McInvaille

Technical Lead - Envista Forensics

Figures

1 - 5

Figure 1.



II. Information to Be Provided by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts, which will be reviewed by law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of 18 U.S.C. section 2114(a), Robbery of a U.S. Postal Service Employee.

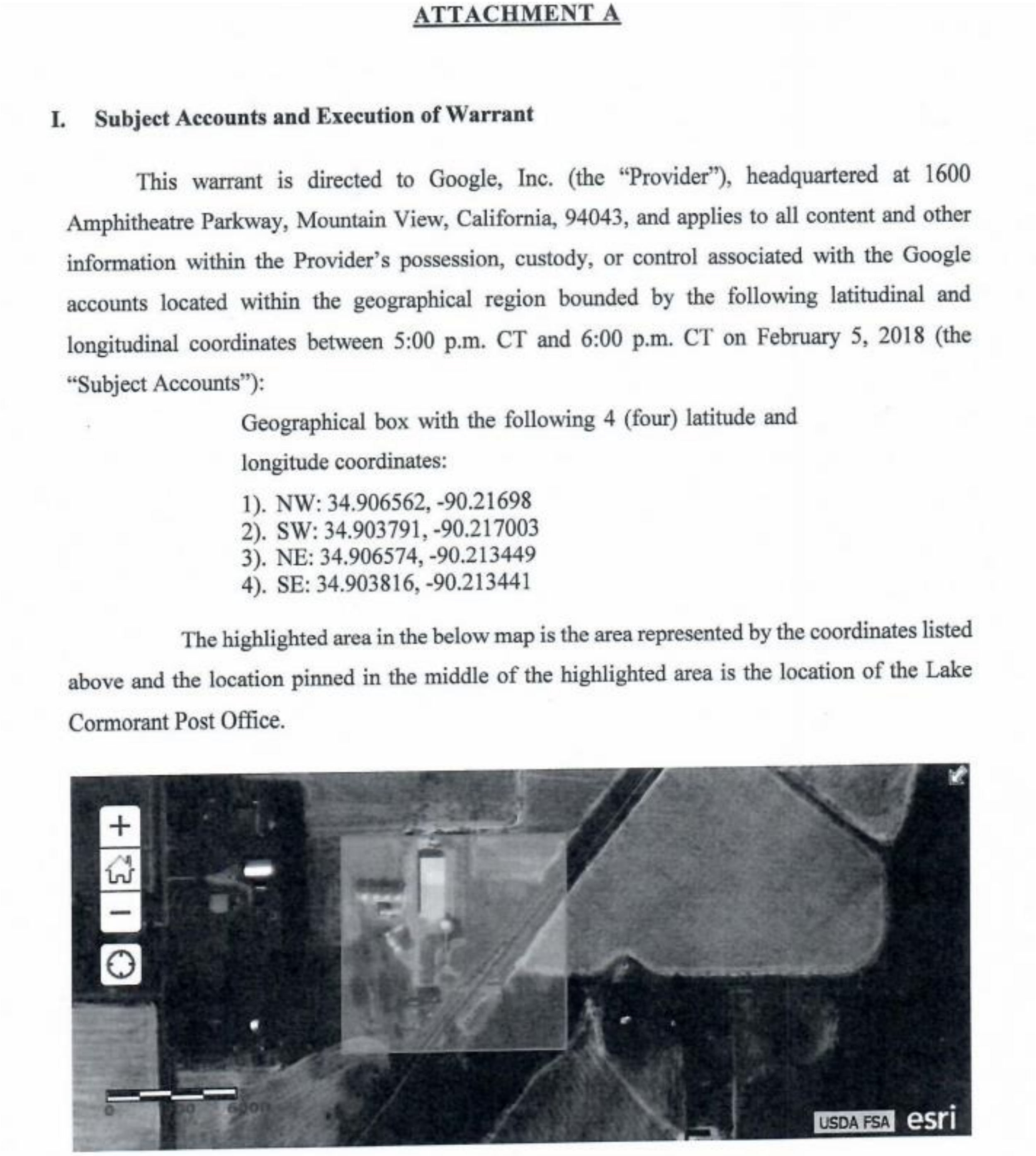
1. *Location information.* All location data, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location, including the GPS coordinates, estimated radius, and the dates and times of all location recordings, **between 5:00 p.m. CT and 6:00 p.m. CT on February 5, 2018**;

2. Any user and each device corresponding to the location data to be provided by the "Provider" will be identified only by a numerical identifier, without any further content or information identifying the user of a particular device. Law enforcement will analyze this location data to identify users who may have witnessed or participated in the Subject Offenses and will seek any additional information regarding those devices through further legal process.

3. For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, the "Provider" shall provide additional location history outside of the predefined area for those relevant accounts to determine path of travel. This additional location history shall not exceed 60 minutes plus or minus the first and last timestamp associated with the account in the initial dataset. (The purpose of path of travel/contextual location points is to eliminate outlier points where, from the surrounding data, it becomes clear the reported point(s) are not indicative of the device actually being within the scope of the warrant.)

4. For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, the "Provider" shall provide the subscriber's information for those relevant accounts to include, subscriber's name, email addresses, services subscribed to, last 6 months of IP history, SMS account number, and registration IP.

Figure 1 cont.



ATTACHMENT A

I. Subject Accounts and Execution of Warrant

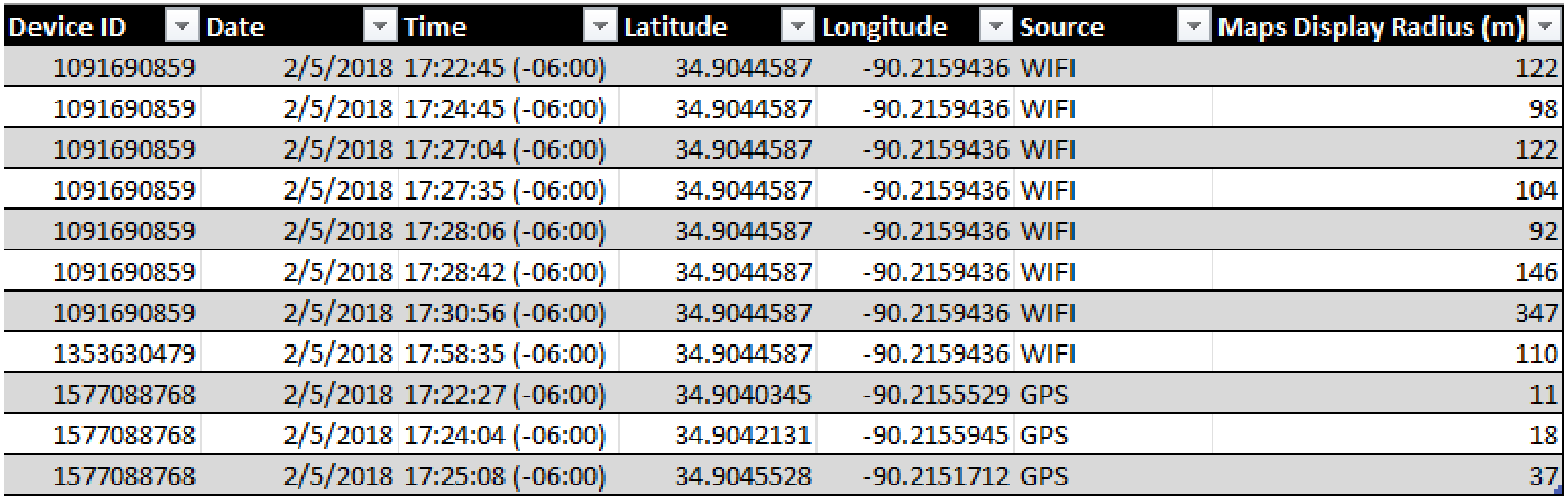
This warrant is directed to Google, Inc. (the "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043, and applies to all content and other information within the Provider's possession, custody, or control associated with the Google accounts located within the geographical region bounded by the following latitudinal and longitudinal coordinates between 5:00 p.m. CT and 6:00 p.m. CT on February 5, 2018 (the "Subject Accounts"):

Geographical box with the following 4 (four) latitude and longitude coordinates:

1). NW: 34.906562, -90.21698
2). SW: 34.903791, -90.217003
3). NE: 34.906574, -90.213449
4). SE: 34.903816, -90.213441

The highlighted area in the below map is the area represented by the coordinates listed above and the location pinned in the middle of the highlighted area is the location of the Lake Cormorant Post Office.

Figure 2.



Device ID	Date	Time	Latitude	Longitude	Source	Maps Display Radius (m)
1091690859	2/5/2018	17:22:45 (-06:00)	34.9044587	-90.2159436	WIFI	122
1091690859	2/5/2018	17:24:45 (-06:00)	34.9044587	-90.2159436	WIFI	98
1091690859	2/5/2018	17:27:04 (-06:00)	34.9044587	-90.2159436	WIFI	122
1091690859	2/5/2018	17:27:35 (-06:00)	34.9044587	-90.2159436	WIFI	104
1091690859	2/5/2018	17:28:06 (-06:00)	34.9044587	-90.2159436	WIFI	92
1091690859	2/5/2018	17:28:42 (-06:00)	34.9044587	-90.2159436	WIFI	146
1091690859	2/5/2018	17:30:56 (-06:00)	34.9044587	-90.2159436	WIFI	347
1353630479	2/5/2018	17:58:35 (-06:00)	34.9044587	-90.2159436	WIFI	110
1577088768	2/5/2018	17:22:27 (-06:00)	34.9040345	-90.2155529	GPS	11
1577088768	2/5/2018	17:24:04 (-06:00)	34.9042131	-90.2155945	GPS	18
1577088768	2/5/2018	17:25:08 (-06:00)	34.9045528	-90.2151712	GPS	37

Figure 3.

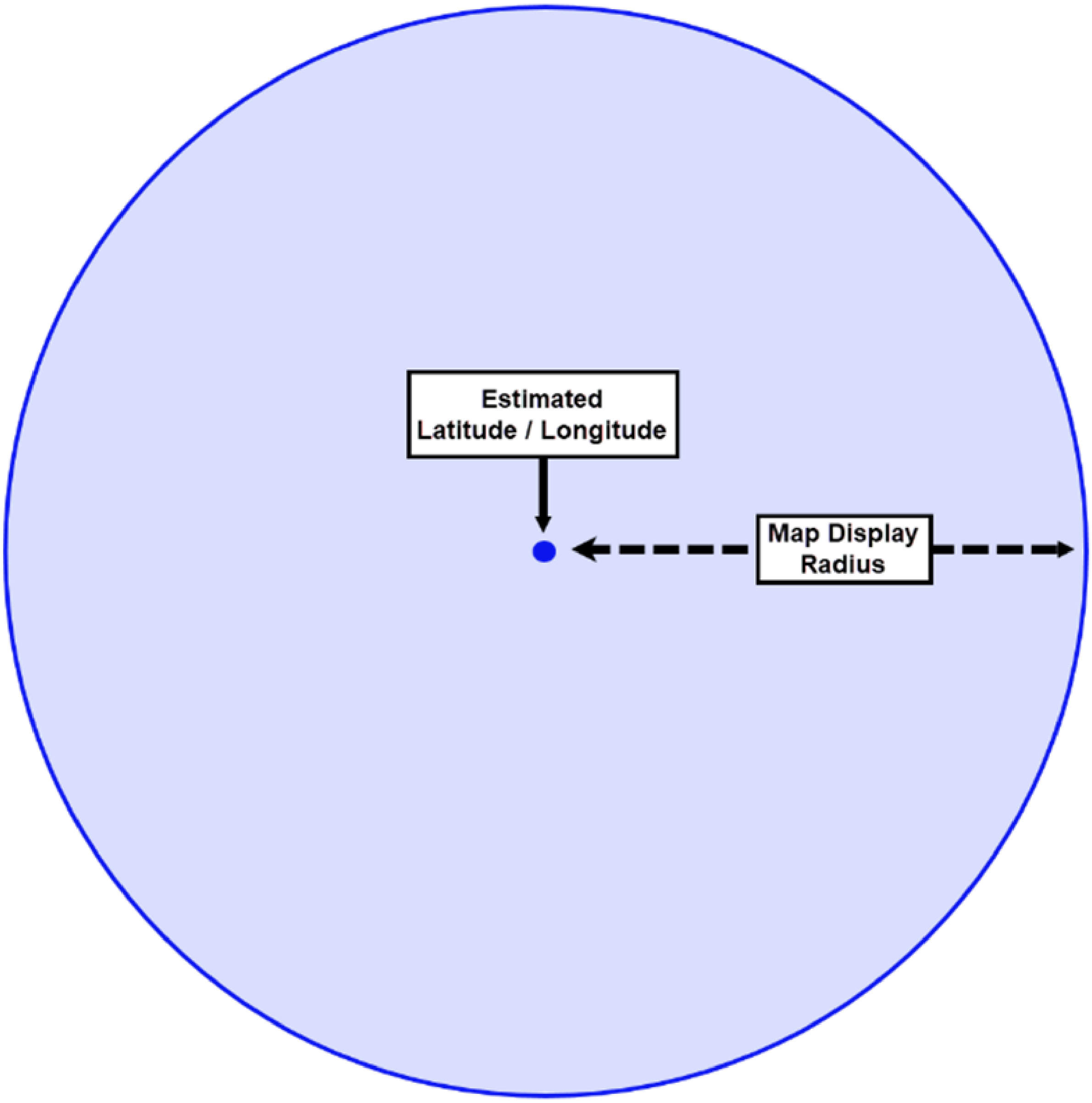


Figure 4.

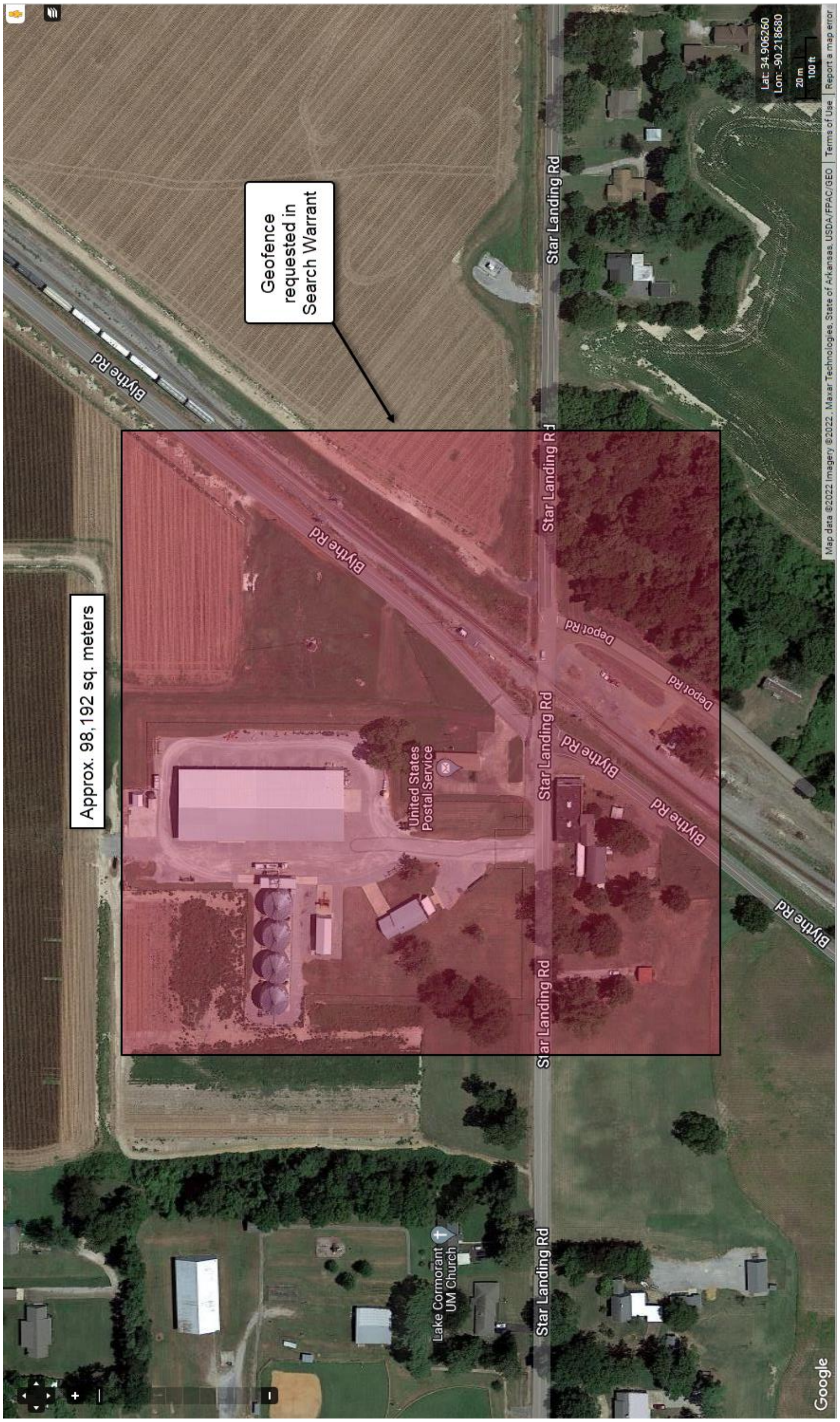
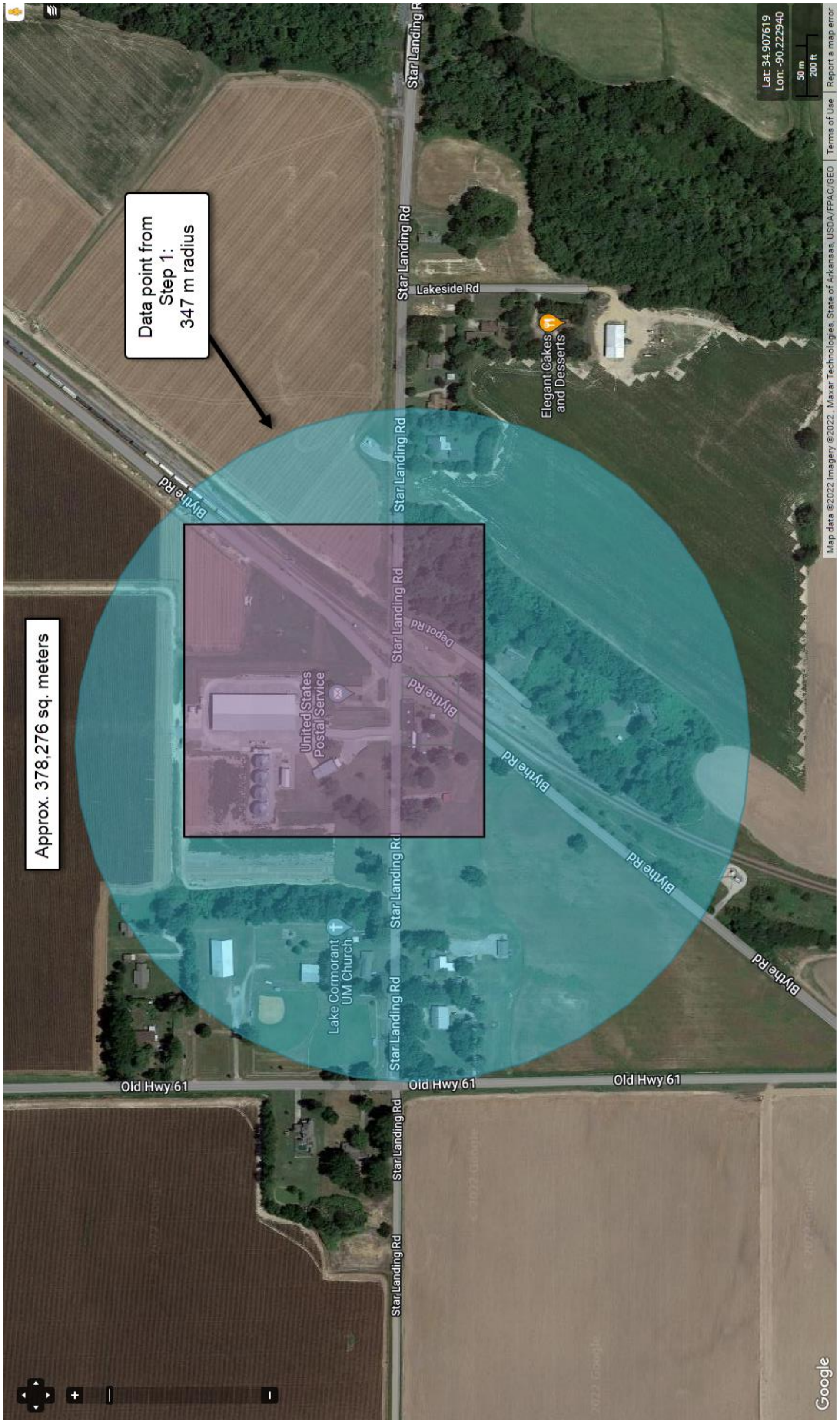

Geofence requested in Search Warrant
Approx. 98,192 sq. meters
Star Landing Rd
Blythe Rd
Depot Rd
United States Postal Service
Lake Cormorant UM Church
Lat: 34.906260
Lon: -90.218680
20 m
100 ft
Map data ©2022 Imagery ©2022 , Maxar Technologies, State of Arkansas, USDA/FPAC/GEO
Terms of Use
Report a map error
Google

Figure 5.


Data point from Step 1: 347 m radius
Approx. 378,276 sq. meters
Star Landing Rd
Lakeside Rd
Elegant Cakes and Desserts
Blythe Rd
Depot Rd
United States Postal Service
Lake Cormorant UM Church
Old Hwy 61
Lat: 34.907619
Lon: -90.222940
50 m
200 ft
Map data ©2022 Imagery ©2022 , Maxar Technologies, State of Arkansas, USDA/FPAC/GEO
Terms of Use
Report a map error
Google

Attachments

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA

v.

OKELLO T. CHATRIE,

Defendant.

Case No. 3:19-cr-00130-MHL

DECLARATION OF MARLO MCGRIFF

I, Marlo McGriff, respectfully submit this declaration in regard to the above-captioned matter. I make this declaration based on my knowledge of the facts stated herein.

1. I am a Location History Product Manager at Google, where my responsibilities include the Location History product. I joined Google in 2011 and have been in my current role since 2016.

2. I lead the cross-functional Location History team and am the overall Location History lead, setting the near-term goals and long-term strategy for the product.

I. Google Location History

3. Some Google services require a user to have a Google account before she can use the service at all, like Gmail. Other services do not require a user to have an account, but offer additional functionality that is only available to Google account holders, like Maps and Search.

4. Google Location History ("LH") is a service that Google account holders may choose to use to keep track of locations they have visited while in possession of their compatible

mobile devices. LH is not available to users who do not have a Google account. Users must explicitly opt in to the service.[1]

5. Google users can visualize their LH data through the "Timeline" feature of Google Maps, which operates as a journal that Google users can choose to use to create, edit, and store a record of their movements and travels. The Timeline feature processes the user's LH data to infer semantic location information such as place visits (*e.g.*, visit to a ski resort), activities (*e.g.*, driving), and paths between place visits (*e.g.*, driving from hotel to ski resort), which is then displayed to the user in her Timeline. LH and the Timeline feature thus allow a user to see where she has traveled with her device and when over a given period.

6. Users who opt into and use LH can access other benefits on their Google devices or applications as well. For instance, they can obtain personalized maps or recommendations based on places they have visited, get help finding their phones, and receive real-time traffic updates about their commutes.

7. For Google LH to function and save information about a user's location, the user must take several steps—some tied to her mobile device, some tied to her Google account.[2] First, the user must ensure that the device-location setting on her mobile device is turned on. When the device-location setting is activated, the mobile device automatically detects its own location, which the device ascertains based on GPS and Bluetooth signals, Wi-Fi connections, and cellular networks. Android users can also tailor their devices' location-reporting settings, controlling which sources of information (*e.g.*, GPS, cellular, or Wi-Fi) the device may use to

[1] *See* Google, *Manage Your Location History*, https://support.google.com/accounts/answer/3118687?hl=en (visited Feb. 27, 2020).

[2] *See generally id.*; Google Privacy & Terms, *How is location saved in my Google Account*?, https://policies.google.com/technologies/location-data#how-save (visited Feb. 27, 2020).

determine location, and which applications can access location data. On iOS devices, the user must further configure her mobile device to share location information by granting the required device-level application location permission.

8. However, merely taking the steps described above—steps that are tied to a mobile device—does not on its own enable LH for a user's account. Google does not save LH information about where a particular mobile device has been to a user's account—even when the device-location feature is turned on and (for iOS) the required device-level application location permissions have been granted—unless the user has also taken additional specific steps tied to her account.

9. For one, the user must opt into LH in her account settings and enable "Location Reporting"—a subsetting within LH—for each particular device on which she wants to use LH. And to actually record and save LH data, the user must then sign into her Google account on her device and travel with that device. A single Google account can be associated with multiple devices, and the "Location Reporting" feature within LH allows users to select the specific devices on which they wish to enable LH.

10. In sum, LH functions and saves a record of the user's travels only when the user opts into LH as a setting on her Google account, enables the "Location Reporting" feature for at least one mobile device, enables the device-location setting on that mobile device (and for iOS devices provides the required device-level application location permission), powers on and signs into her Google account on that device, and then travels with it.

11. When a user takes the above-mentioned steps, the resulting data is communicated to Google for processing and storage. Google stores this data in a database internally referred to as "Sensorvault." Only LH information is stored in Sensorvault.

12. LH information may be considerably more precise than other kinds of location data, including cell-site location information ("CSLI"). That is because, as a technological matter, a mobile device's location-reporting feature can use multiple inputs in estimating the device's location. Those inputs could include GPS signals (*i.e.*, radio waves detected by a receiver in the mobile device from orbiting geolocation satellites) or signals from nearby Wi-Fi networks, Bluetooth beacons, or cell towers. Combined, these inputs (when the user enables them) can be capable of estimating a device's location to a higher degree of accuracy and precision than is typical of CSLI. For example, I understand that when a strong GPS signal is available, a device's location can be estimated within approximately twenty meters or less.

13. In 2019, the majority of Google users worldwide did not have LH enabled on their account. While a more precise percentage is difficult to calculate in part due to fluctuating numbers of users, in 2019, roughly one-third of active Google users (i.e., numerous tens of millions of Google users) had LH enabled on their accounts.

14. Depending on a user's ads personalization setting, Google may use the semantic location information described in Paragraph 5 above (*e.g.*, place visits) that the Timeline feature infers from LH to show relevant ads to the user. For example, a user who regularly frequents ski resorts may later see an ad for ski equipment when watching a video on YouTube. Additionally, Google may also use the semantic location information that the Timeline feature infers from LH in an anonymized and aggregated manner to help advertisers measure how often an online ad campaign helps drive traffic to physical stores or properties. Google does not share LH or any other information identifying individual users with advertisers.[3] Additionally, at all times

[3] *See* Google Privacy & Terms, *How is location used to show ads?*, https://policies.google.com/technologies/location-data#show-ads (visited Feb. 27, 2020).

relevant to this warrant, Google has not shared identified LH data with third parties except through legal process and has not monetized identified LH data.

15. Critically, as described in Google's Privacy Policy at https://policies.google.com/technologies/retention, a user remains in control of her LH data through her Timeline. She can review, edit, or delete her Timeline at will. By deleting Timeline entries, a user also deletes the underlying LH information. As such, the user could decide to keep LH information only for certain dates; she could delete all LH information except those associated with certain Timeline entries; she could instruct Google to automatically delete all LH information after a set period; or she could keep all LH information for future reference. When a user deletes data in her Google account, Google immediately starts the process of removing it from the product and our systems as described in Google's Privacy Policy, at https://policies.google.com/technologies/retention.

16. Google users may also opt into a separate service called Web & App Activity ("WAA"). If a user turns on the WAA setting in his or her Google account with the necessary app-level and device-level permissions (*e.g.*, if the device-location setting on the mobile device is active), some activities that the user engages in while logged into her account (for instance, Google searches) are saved to that account, so the user may have a more personalized experience. For example, she may experience faster searches and more helpful app and content recommendations, such as when a user sees her search automatically suggested based on past searches.[4] Some of these WAA entries can include location information, although the source of

[4] *See, e.g.*, Google, *See & control your Web & App Activity*, https://support.google.com/websearch/answer/54068?co=GENIE.Platform%3DAndroid&hl=en (visited Feb. 27, 2020); Google Privacy & Terms, *How is location saved in my Google Account?, at Web & App Activity*, https://policies.google.com/technologies/location-data#how-save (visited Feb. 27, 2020).

the location information will vary depending on the activity, the device, and the user's other settings. LH and WAA are separate services that store data in separate databases, and there are no dependencies between LH and WAA. WAA data is not used to calculate the locations that are stored in LH, and completing a search across LH data does not search or draw on WAA data in any way.

17. Google Location Accuracy ("GLA") is a separate setting, which was formerly known as Google Location Services. It is available only on Android mobile devices. When the GLA setting is turned off, an Android device will use only GPS data to calculate its location. If a user has the GLA setting on, the Android's location services will use additional inputs, including Wi-Fi access points, mobile networks, and sensors, to estimate the device's location.[5] While location data may be periodically collected from devices with the GLA setting turned on and used in an anonymous way to improve location accuracy (*e.g.*, estimating the locations of WiFi access points and cell towers), that location data is not stored with user identifiers and is stored separately from the LH database and the WAA database.[6] As indicated, if a user has turned on GLA, then the device's location information that is sent to and stored in LH (if LH has been enabled) may be calculated using not only GPS-sourced data, but also WiFi- or cell-sourced data from the GLA database. In other words, GLA data might be used by the device to calculate a location data point that is then stored in LH. But there are no other dependencies between GLA and LH. Completing a search across LH data does not search or draw on GLA data in any way—the databases are separate and do not interact beyond the initial location calculation.

[5] *See, e.g.*, Google, *Manage your Android device's location settings*, https://support.google.com/nexus/answer/3467281?hl=en (visited Feb. 27, 2020).

[6] *See, e.g.*, Google Privacy & Terms, *How does Google know my location?*, at Google Location Services, https://policies.google.com/technologies/location-data (visited Feb. 27, 2020).

18. When GLA is turned on, the inputs used to calculate a user's estimated location can include WiFi access points. However, Google cannot reconstruct which WiFi access points were used to calculate a given LH data point. Although Google collects anonymized data in GLA that allows it to estimate the physical location of particular WiFi access points, and those WiFi access points in turn can be an input used to calculate a device's estimated location that is then stored in LH, Google does not know and cannot recreate which particular WiFi access points were used to calculate any particular LH data point. Google therefore cannot identify the physical location of the WiFi access points used to estimate a user's location coordinates stored in LH because it cannot determine which WiFi access points were used to estimate the user's location.

II. Google's Production of LH Information to Law Enforcement

19. I understand that this case concerns a so-called "geofence" request, which seeks LH information for all Google users whose LH information indicates that their device may have been present in a specified geographic area during a certain window of time.

20. In practice, LH is the only form of location data Google maintains that Google believes to be responsive to a geofence request, and LH is the only form of location data that was produced to the government in this case. This is because at all times relevant to this case, Google has not stored any other location information in association with specific Google user accounts that is sufficiently granular to be responsive to and searchable for such a request. To be relevant and responsive to a geofence warrant, location data must be stored in association with a specific user's account and must be able to pinpoint a user's estimated location with enough precision to bring it within the radius described in a geofence warrant. Even though Google devices and applications might sometimes use or transmit information about a user's location to

Google while the device or application is in use, no such information other than LH is stored and searchable in association with specific user accounts at a level of precision sufficient to be searched and produced in response to a geofence warrant.

21. At all times relevant to this case, WAA did not store a user's location at a level of detail precise enough to be responsive to a geofence warrant. Stored WAA data reflects a device's location to an approximate area of at least one square kilometer; and, if there are fewer than 1000 users in one square kilometer, the area is even larger. WAA data was therefore too coarse to be responsive to the warrant in this case and was not searched or produced.

22. Google does not store GLA data in association with any particular Google account. GLA data therefore is not responsive to a typical geofence warrant and was not responsive or relevant to the warrant in this case and was not searched or produced.

23. LH information can be searched in response to a geofence request. To conduct that search, Google must search across *all* LH data to identify users with LH data during the relevant timeframe, and run a computation against every set of stored LH coordinates to determine which records match the geographic parameters in the warrant. Google does not know which users may have such saved LH data before conducting the search and running the computations.

24. The location data points reflected in LH are estimates based on multiple inputs, and therefore a user's actual location does not necessarily align perfectly with any one isolated LH data point. Each set of coordinates saved to a user's LH includes a value, measured in meters, that reflects Google's confidence in the saved coordinates. A value of 100 meters, for example, reflects Google's estimation that the user is likely located within a 100-meter radius of the saved coordinates based on a goal to generate a location radius that accurately captures

roughly 68% of users. In other words, if a user opens Google Maps and looks at the blue dot indicating Google's estimate of his or her location, Google's goal is that there will be an estimated 68% chance that the user is actually within the shaded circle surrounding that blue dot.

25. Notwithstanding the confidence interval described above, if a user's estimated location (*i.e.*, the stored coordinates in LH) falls within the radius of the geofence request, then Google treats that user as falling within the scope of the request, even if the shaded circle defined by the 68% confidence interval falls partly outside the radius of the geofence request. As a result, it is possible that when Google is compelled to return data in response to a geofence request, some of the users whose locations are estimated to be within the radius described in the warrant (and whose data is therefore included in a data production) were in fact located outside the radius. To provide information about that, Google includes in the production to the government a radius (expressed as a value in meters) around a user's estimated location that shows the range of location points around the stored LH coordinates that are believed to contain, with 68% probability, the user's actual location.

26. In contrast, the purposes for which Google designed LH do not depend on any individual stored LH data points. For instance, the Timeline feature combines and contextualizes numerous individual stored LH data points over periods of time into inferred semantic location information (*e.g.*, place visits) so that users may store and visualize their location and movements in a journal (*e.g.*, visiting a hotel, visiting a ski resort, and driving between that hotel and ski resort). Similarly, Google may use such inferred semantic place visits (not individual stored LH data points) for ads. LH is sufficiently precise and reliable for these purposes for which Google designed LH.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 11th day of MAR 2020, in San Francisco.

Marlo McGriff

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
RICHMOND DIVISION

UNITED STATES OF AMERICA

v.

OKELLO T. CHATRIE,

Defendant.

Case No. 3:19-cr-00130-MHL

DECLARATION OF SARAH RODRIGUEZ

I, Sarah Rodriguez, respectfully submit this declaration in regard to the above-captioned matter. I make this declaration based on my knowledge of the facts stated herein.

1. I am a Team Lead for Legal Investigations Support (LIS) at Google, where my responsibilities include processing law enforcement legal process requests directed at Google, including requests for Location History (LH) information. I joined Google in 2011 and have been in my current role since March 2018.

2. In my position, I am responsible for managing a team of LIS specialists who process and respond to certain law enforcement requests for data, including the LIS specialists involved in processing the search warrant in this case. I also process and respond to these requests.

I. Google's Production of LH Information to Law Enforcement In Response To Geofence Warrants

3. Google often receives search warrants from law enforcement authorities in the United States for a specifically identified Google user's Location History ("LH") information from a specifically identified time range. When producing data in response to such a demand,

Google searches for and retrieves only the responsive data that is associated with the particular users or accounts identified in the warrant.

4. Google also often receives search warrants from law enforcement in the United States for so-called "geofence" requests. Typically, such requests do not specify any known person, user, or account. Instead, geofence requests seek LH information for all Google users whose LH information indicates that their devices may have been present in a specified geographic area surrounding a point of interest, which law enforcement often indicates is a suspected crime scene, and a certain window of time, which might span a few minutes or a few hours.

5. Early "geofence" legal requests sought LH data that would identify all Google users who were in a geographical area in a given time frame. To ensure privacy protections for Google users and to protect against overbroad disclosures based on non-contextualized LH information, Google instituted a policy of objecting to any warrant that failed to include deidentification and narrowing measures. That protocol typically, as included in the search warrants, entails a three-step process.

6. First, law enforcement generally obtains a search warrant compelling Google to disclose a deidentified list of all Google user accounts for which there is saved LH information in a defined geographic area during a defined timeframe.

7. To comply with this first step of the process, Google must conduct the search across *all* LH data to identify users with LH data during the relevant timeframe, and run a computation against every set of stored LH coordinates to determine which records match the geographic parameters in the warrant. Google does not know which users may have such saved LH data before conducting the search and running the computations.

8. After that search is completed, LIS assembles the stored LH records responsive to the request without any account-identifying information. This deidentified "production version" of the data includes a device number, the latitude/longitude coordinates and timestamp of the stored LH information, the map's display radius, and the source of the stored LH information (that is, whether the location was generated via Wi-Fi, GPS, or a cell tower). The volume of data produced at this stage depends on the size and nature of the geographic area and length of time covered by the geofence request, which vary considerably from one request to another. LH records are deemed responsive to a geofence warrant (*i.e.*, a user's estimated location is treated as falling within the scope of the warrant) if the stored latitude/longitude coordinates fall within the radius described in the warrant. That is true even if the shaded blue radius around those coordinates, which I understand reflects a 68% confidence interval around the location estimate, falls in part outside of the radius described in the warrant.

9. LIS deidentifies the data produced to the government at this step by removing the Google Account ID (an internal identification number assigned to the Google account that is associated to the device that is specific to each Google account) associated with the data, leaving only a device number that is used only in the Location History database. This device number is only used for distinguishing devices reporting LH to a user's account, is not a valid account identifier (as it is not unique across accounts), and cannot be mapped to an Android ID, mobile equipment identifier (MEID), or international mobile station equipment identity (IMEI) number (as it is not unique across devices).[1]

[1] An Android ID is an internal identification number assigned to each Android device connected to the Google Services Framework. *See* Google Pixel Phone Help, *Learn about the Android Device Configuration Service*, https://support.google.com/pixelphone/answer/9021432?hl=en (visited Feb. 28, 2020).

10. Second, the government reviews the deidentified production version to determine the device numbers of interest. If additional deidentified location information for a device in the production is necessary to eliminate false positives or otherwise determine whether that device is actually relevant to the investigation, law enforcement can compel Google to provide additional contextual location coordinates beyond the time and geographic scope of the original request (if authorized in that request).

11. This additional contextual LH information can assist law enforcement in eliminating devices in the production that were not in the target location for enough time to be of interest, were moving through the target location in a manner inconsistent with other evidence, or otherwise are not relevant to the investigation.

12. Finally, based on the deidentified data produced, the government can compel Google (if authorized in the request) to provide account-identifying information for the device numbers in the production that the government determines are relevant to the investigation. In response, Google provides account subscriber information such as the email address associated with the account and the name entered by the user on the account.

II. This Geofence Warrant

13. In this case, Google received a geofence warrant (Google Reference No. 2590472) dated June 14, 2019, that was submitted to Google's online system through Detective Joshua Hylton's verified account on June 20, 2019. The geofence warrant requested information about Google accounts associated with devices that reported a location located within a 150-meter radius around a specified latitude and longitude coordinate (described as an area surrounding a Federal Credit Union and located in Richmond, Virginia) between 4:20 P.M. and

5:20 P.M. on Monday, March 20, 2019. The warrant set forth the three-step process (described above), which Google followed.

14. A LIS specialist executed the query for searching across all LH data to identify users with LH data during the specified timeframe and to run the computations against every set of coordinates in order to determine which LH records matched the geographic parameters in the warrant. The LIS specialist then produced the deidentified "production version" of the LH records responsive to the request (*i.e.*, no account-identifying information) through Google's online system to Detective Hylton's online account on or about June 28, 2019. As described above, this production included the latitude/longitude coordinates and timestamp of the responsive stored LH information, along with a display radius around those coordinates (expressed as a distance in meters) that reflects Google's confidence in the LH coordinates. A value of 100 meters, for example, I understand reflects Google's estimation that the user was likely located within a 100-meter radius of the saved coordinates based on a goal to generate a location radius that accurately captures roughly 68% of users. I understand that the same calculation would apply to any other display radius given in the production.

15. On or about July 2, 2019, Google received an email from Detective Hylton requesting additional location data (*i.e.*, step 2) and subscriber information (*i.e.*, step 3) for all 19 device numbers produced in step 1.

16. On or about July 8, 2019, Google received two voicemails from Detective Hylton. A LIS specialist called Detective Hylton that day and explained the issues in the Detective's email as the request did not appear to follow the three sequential steps or the narrowing required by the search warrant. Detective Hylton asked, and the LIS specialist explained, what information would be produced in step 2 and after in step 3. The LIS specialist also explained the importance of step 2 in narrowing. Detective Hylton stated that Google could run step 2 on

the first 9 device numbers in his email, dated July 2, 2019. Detective Hylton also stated that he would attempt to narrow further for step 3.

17. On or about July 9, 2019, Google received an email from Detective Hylton requesting additional location data (*i.e.*, step 2) on 9 device numbers.

18. A LIS specialist executed the query to search for the additional contextual location coordinates for the 9 device numbers beyond the time and geographic scope of the original request (as authorized in the search warrant). The LIS specialist then produced the deidentified "production version" of the LH records responsive to the request (*i.e.*, no account-identifying information) through Google's online system to Detective Hylton's online account on or about July 9, 2019.

19. On or about July 10, 2019, and July 11, 2019, Google received emails from Detective Hylton requesting subscriber information (*i.e.*, step 3) on 3 device numbers.

20. A LIS specialist produced the account subscriber information associated with the 3 device numbers on or about July 11, 2019.

21. On or about July 12, 2019, Google received an email from Detective Hylton requesting additional device or phone number information that could be associated with one of the accounts that LIS produced subscriber information on in step 3. A LIS specialist called Detective Hylton on or about July 12, 2019, and no further information was produced under this search warrant.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 11th day of March 2020, in San Francisco, CA.

Sarah Rodriguez

Lauren J. Tsuji (Bar No. 300155)
LTsuji@perkinscoie.com
John R. Tyler (*pro hac vice*)
RTyler@perkinscoie.com
Anna Mouw Thompson (*pro hac vice*)
AnnaThompson@perkinscoie.com
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
Telephone: 206.359.8000
Facsimile: 206.359.9000

Attorneys for Non-Party Google LLC

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF SAN FRANCISCO

PEOPLE OF THE STATE OF CALIFORNIA

Plaintiff,

v.

LAQUAN DAWES,

Defendant.

Case No. 19002022

DECLARATION OF EMILY MOSELEY

DECLARATION OF EMILY MOSELEY

I, Emily Moseley, respectfully submit this declaration in regard to the above-captioned matter. I make this declaration based on my knowledge of the facts stated herein.

1. I am a Policy Specialist at Google LLC ("Google"), where my responsibilities include processing law enforcement legal process requests directed at Google, including requests for Location History (LH) information. I joined Google in 2019 and have been in my current role ever since.

2. In my position, I am responsible for processing and responding to law enforcement requests for Location History, as well as ensuring that productions are complete and contain the correct records. I am also responsible for resolving escalations that arise from law enforcement requests for Location History.

Location History in October 2018

3. In October 2018, there were approximately 592 million daily active users of Location History worldwide. Roughly one-third of all active Google users had Location History enabled on their accounts.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed this 4th day of May, 2022, at Mountain View, California.

s/ Emily Moseley
Emily Moseley